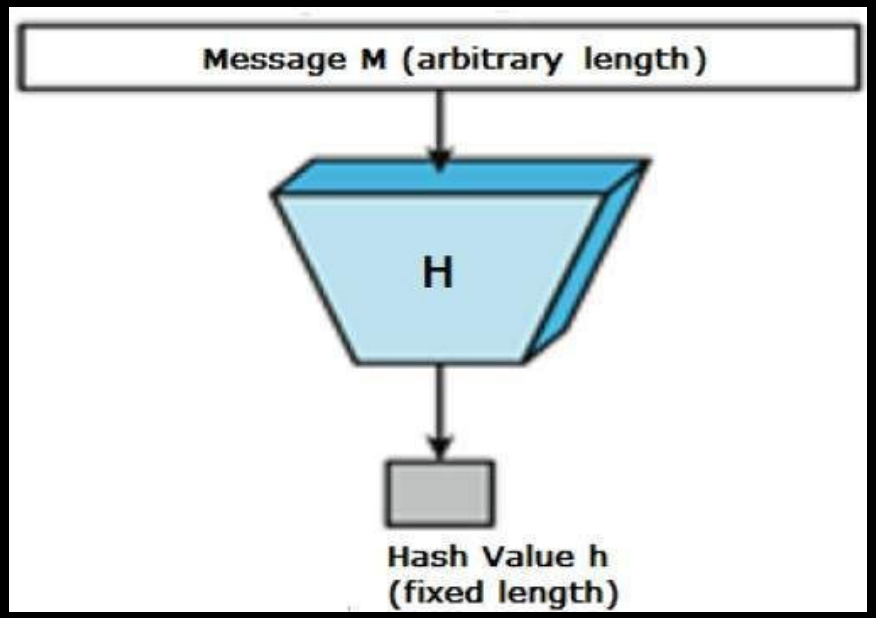
인공지능 보안

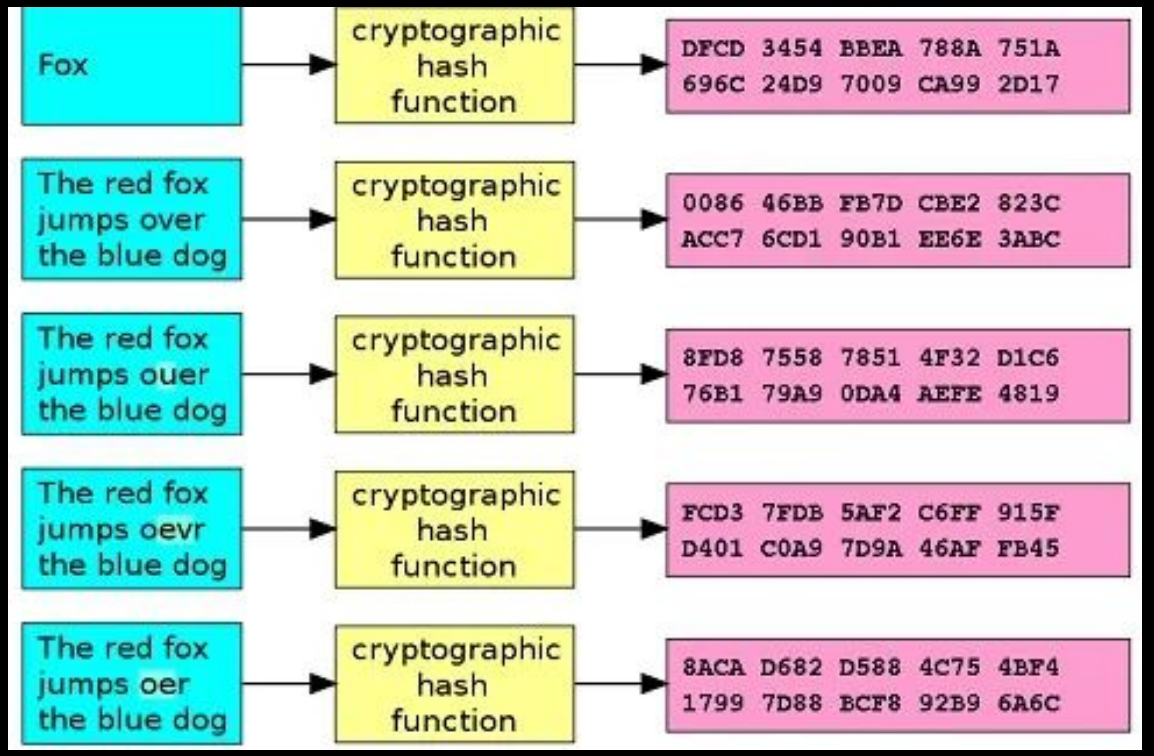
-09-

네트워크 보안

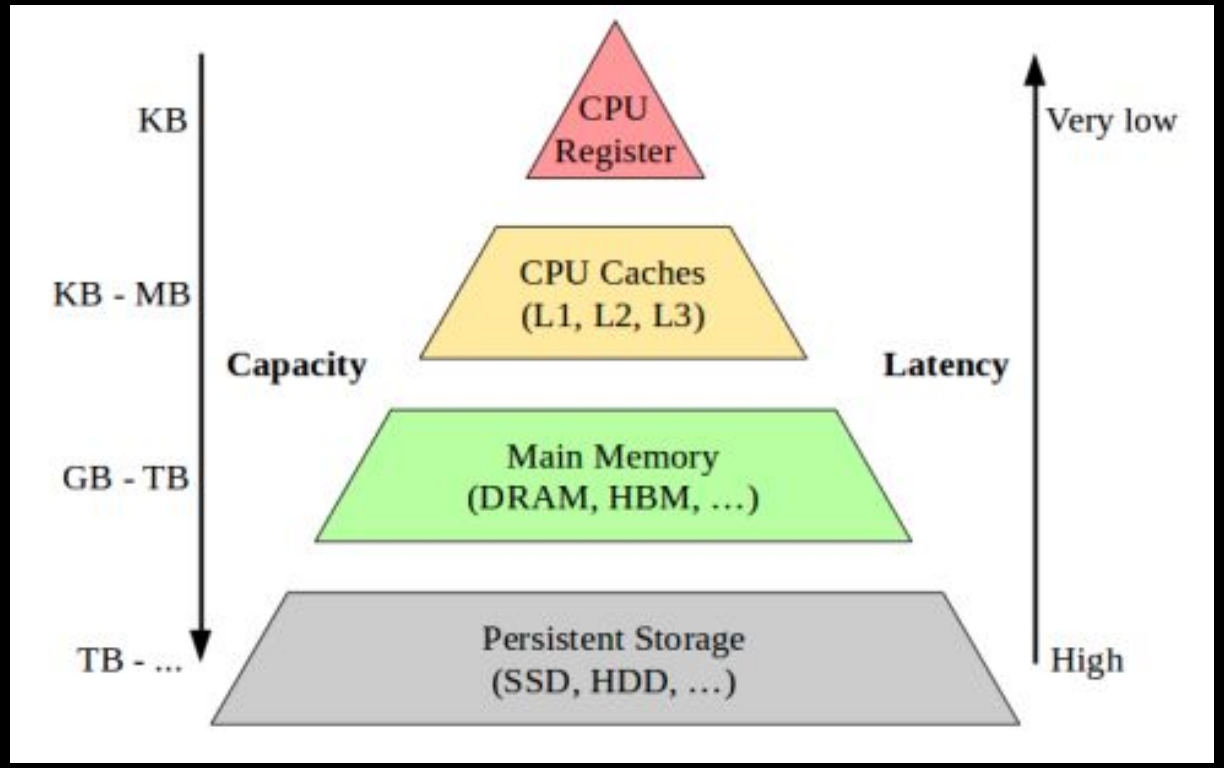
Hash

Hash Function

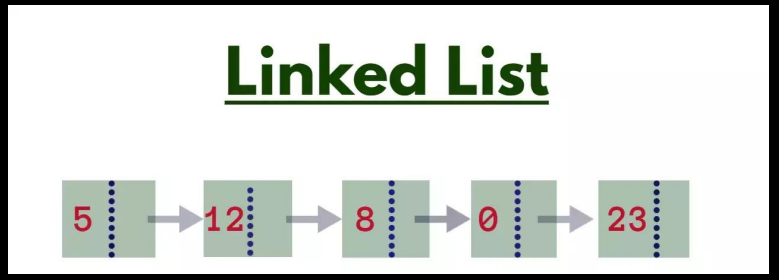


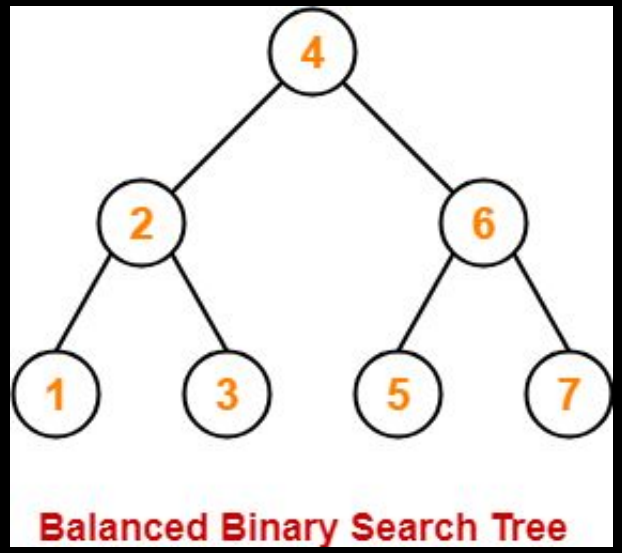


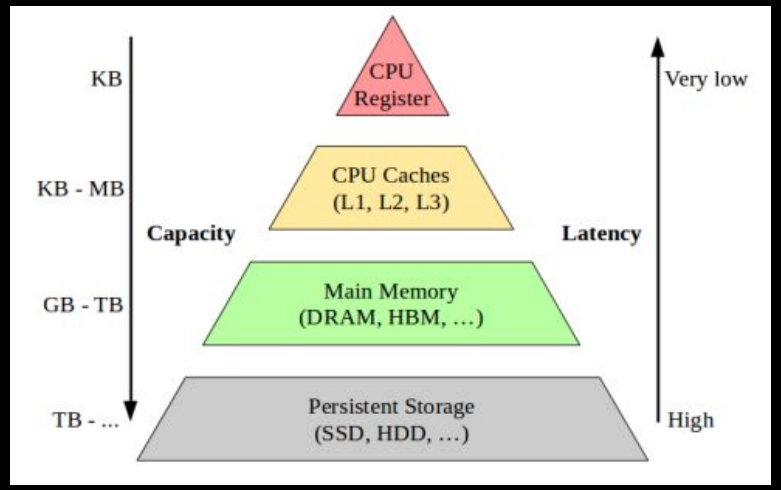
Memory Hierarchy



Complexity


Linked List
5
12
8
0
23

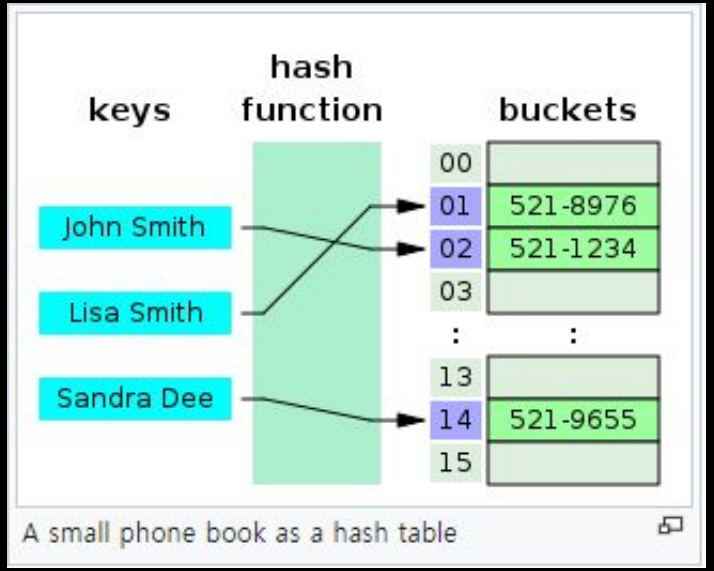

4
2
6
1
3
5
7
Balanced Binary Search Tree


KB
KB - MB
GB - TB
TB - ...
Capacity
CPU Register
CPU Caches (L1, L2, L3)
Main Memory (DRAM, HBM, …)
Persistent Storage (SSD, HDD, …)
Latency
Very low
High

Hash Table

- The advantage of using hashing is that the table address of a record can be directly computed from the key

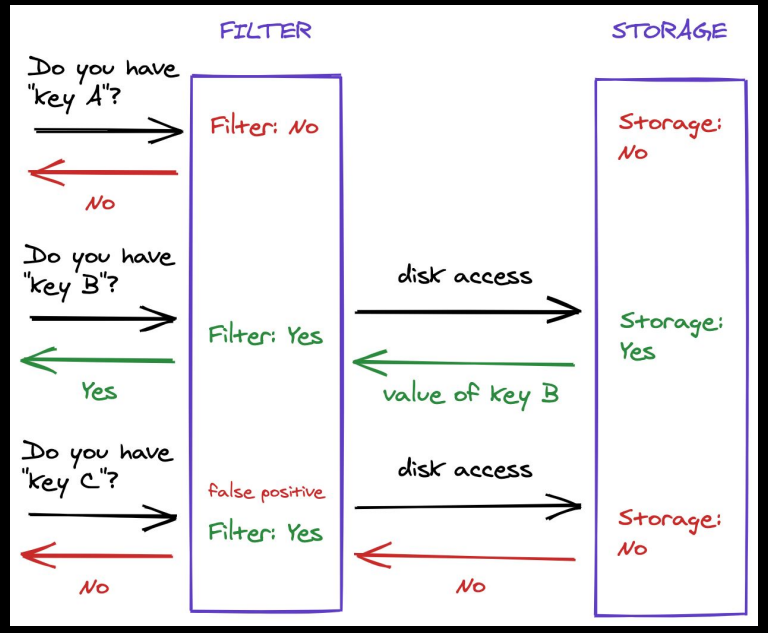
- Hash functions should provide a uniform distribution of hash values
- Cryptographic hash functions are believed to provide good hash functions for any table size, either by modulo reduction or by bit masking



$$\text{Hash} = \text{Hash-Function(Key)}$$
$$\text{Index} = \text{Hash} \ \% \ \text{Hash-Table-Size}$$

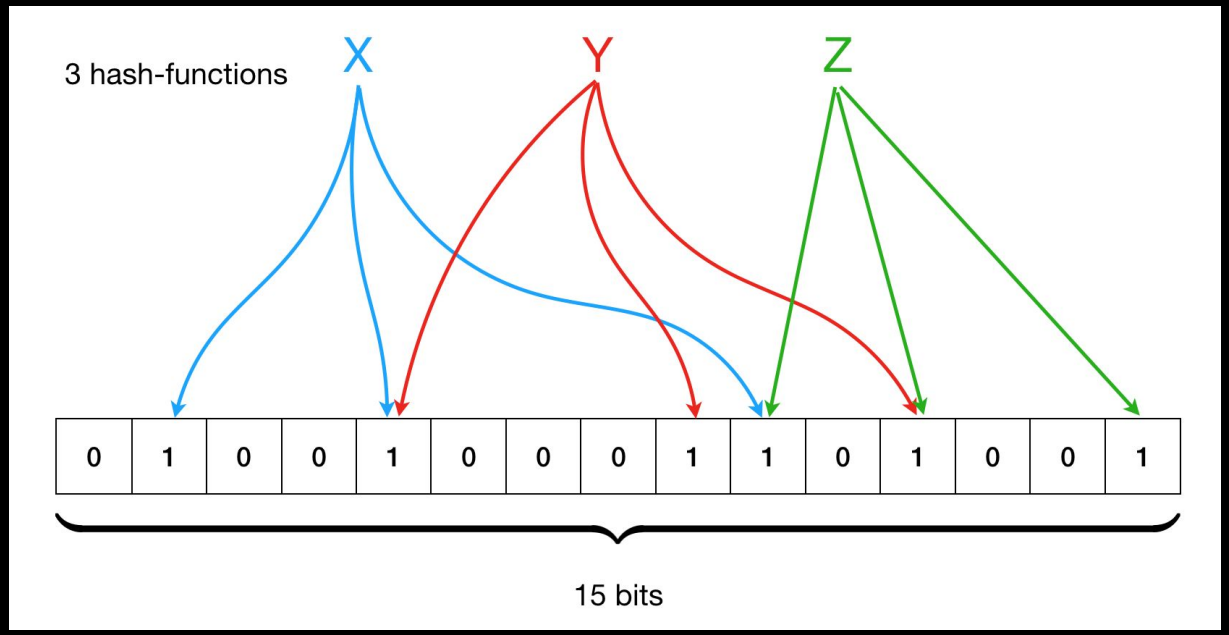
Bloom Filter

Bloom Filter



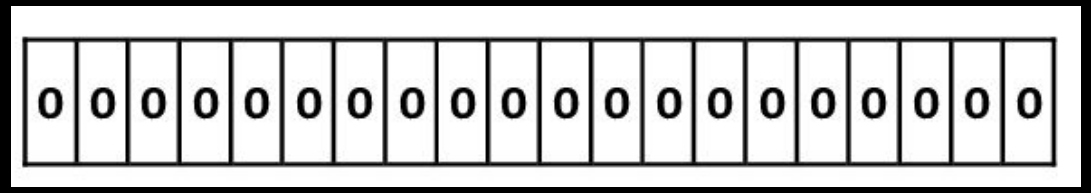
A space-efficient probabilistic data structure that is used to test whether an element is a member of a set.
False positive matches are possible, but false negatives are not - in other words, a query returns either "possibly in set" or "definitely not in set".

Bloom Filter

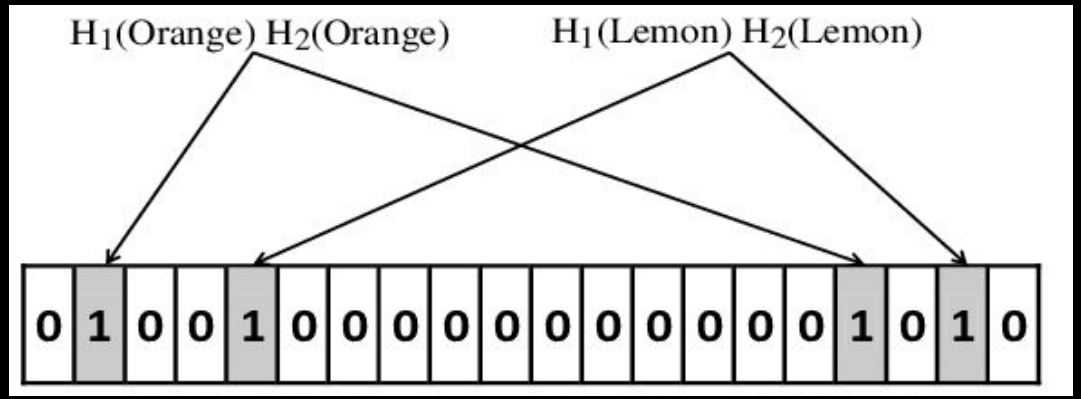


bit array of size m(15)
k(3) of different hash-functions

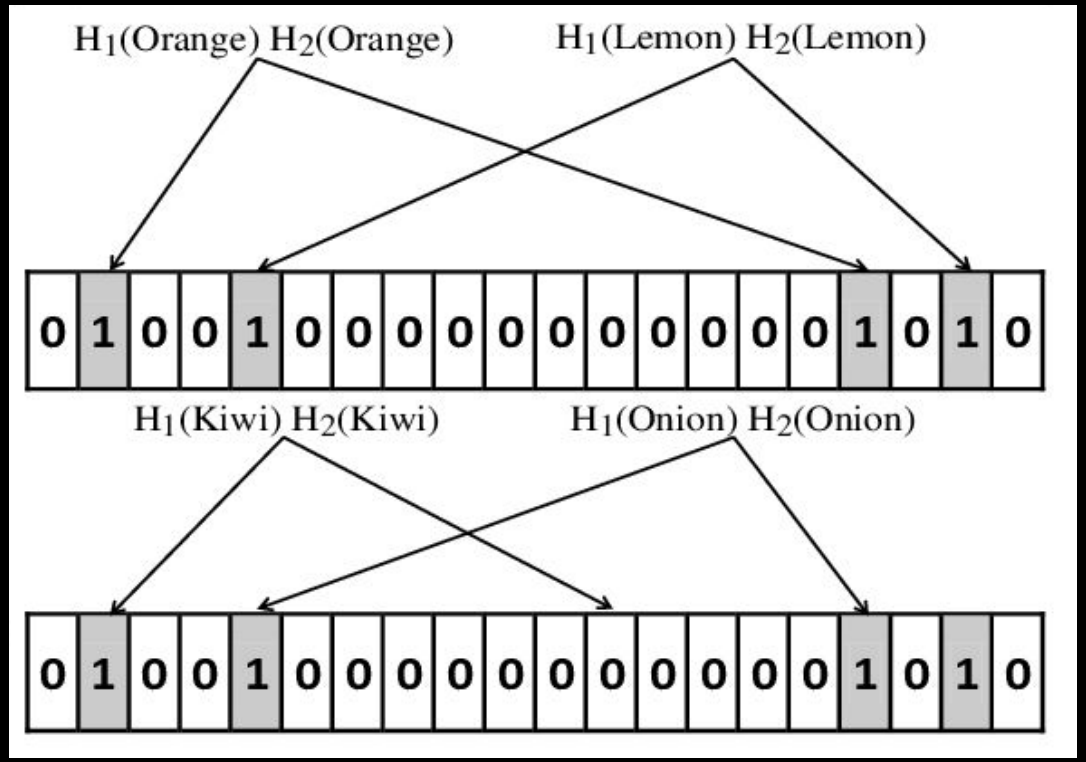
Bloom Filter : Initialize



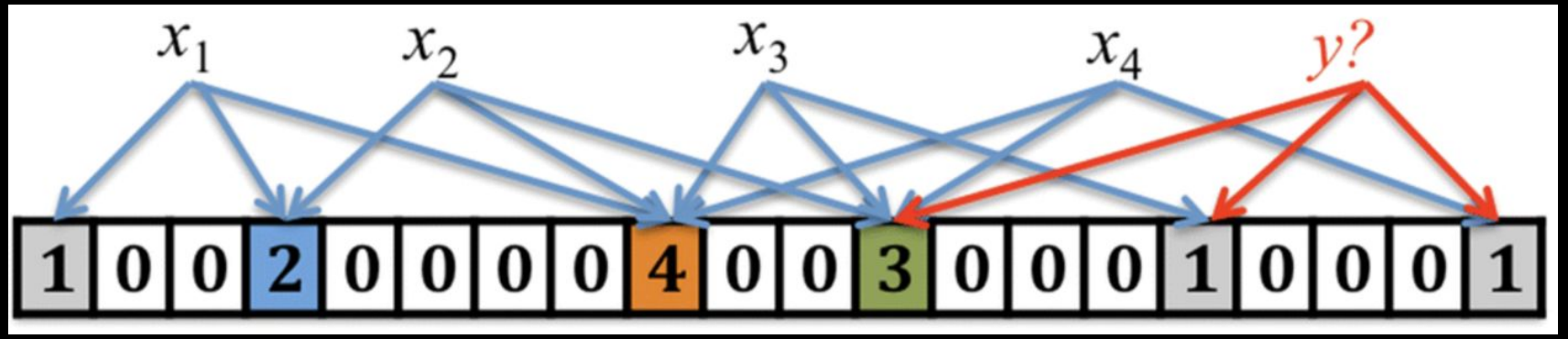
Bloom Filter : Insert



Bloom Filter : Query



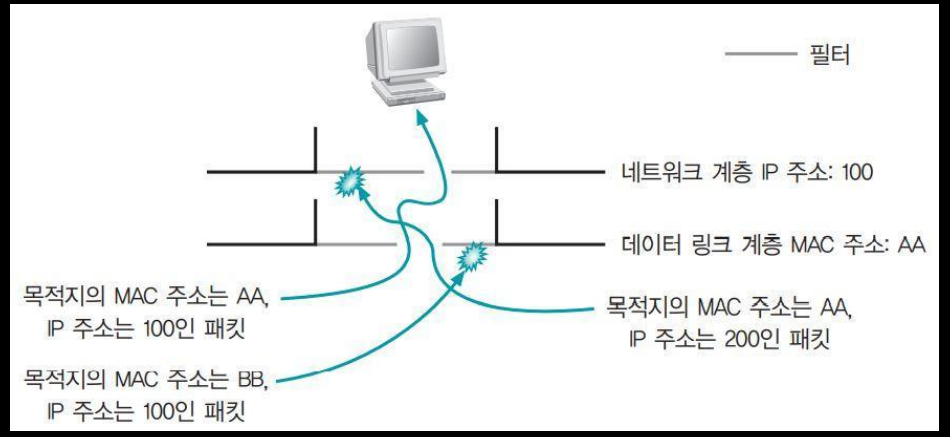
Counting Bloom Filter



스니핑 & 스푸핑

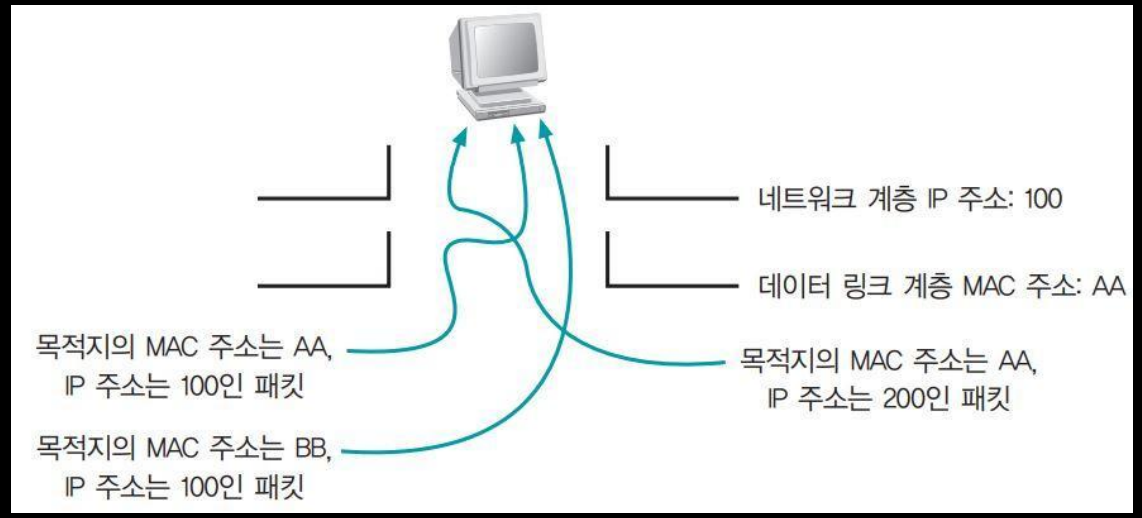
스니핑 공격

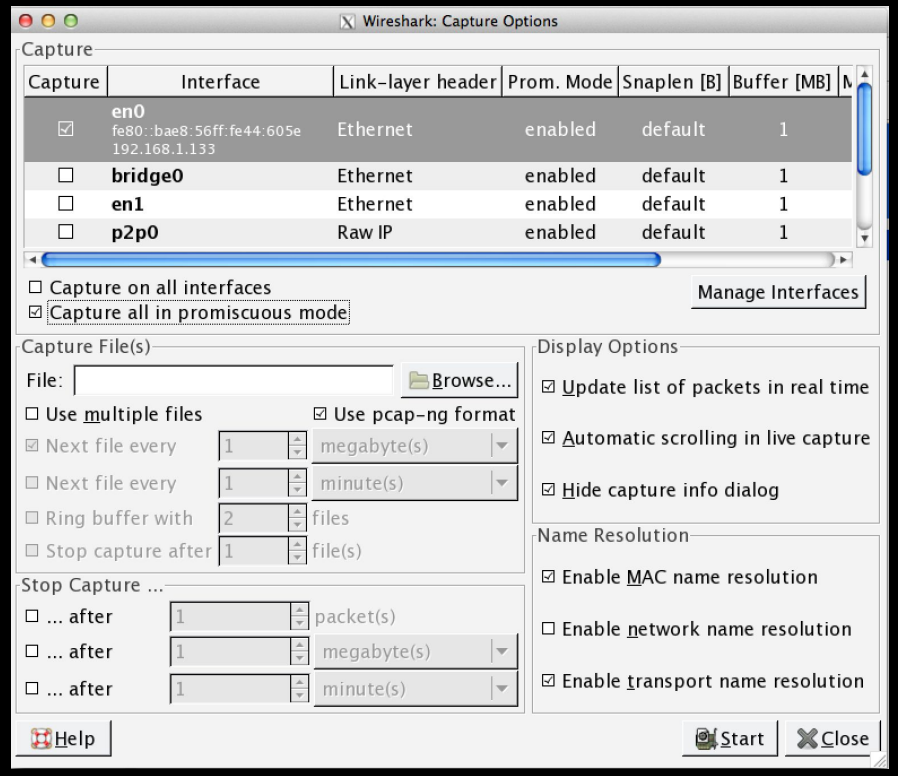
- 스니핑 공격의 개요
  - 공격할 때 아무것도 하지 않고 조용히 있는 것만으로도 충분하기 때문에 수동적 공격이라고도 함
  - 다른 사람의 대화를 엿듣거나 도청하는 행위
- 스니핑 공격의 원리
  - 네트워크 카드는 패킷의 IP 주소와 MAC 주소를 인식하고 자신의 버퍼에 저장할지를 결정
  - 네트워크 카드에 인식된 데이터 링크 계층과 네트워크 계층의 정보가 자신의 것과 일치하지 않는 패킷은 무시



스니핑 공격

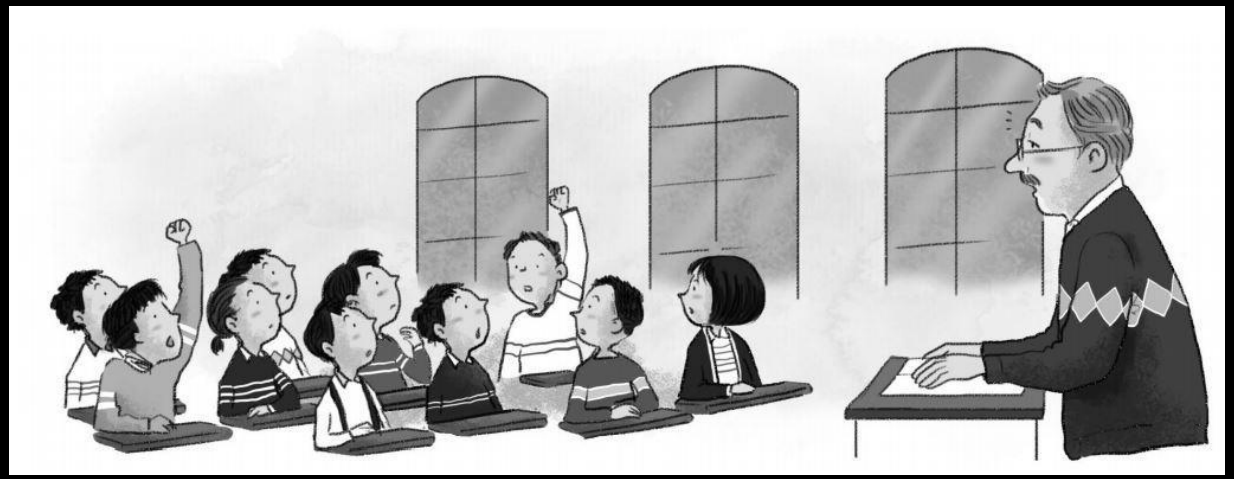
- 랜 카드의 설정 사항을 간단히 조정하거나 스니핑을 위한 드라이버를 설치하여 무차별 모드로 변경
- 무차별 모드 (Promiscuous mode): 데이터 링크 계층과 네트워크 계층의 필터링을 해제하는 랜 카드의 모드





스니핑 공격

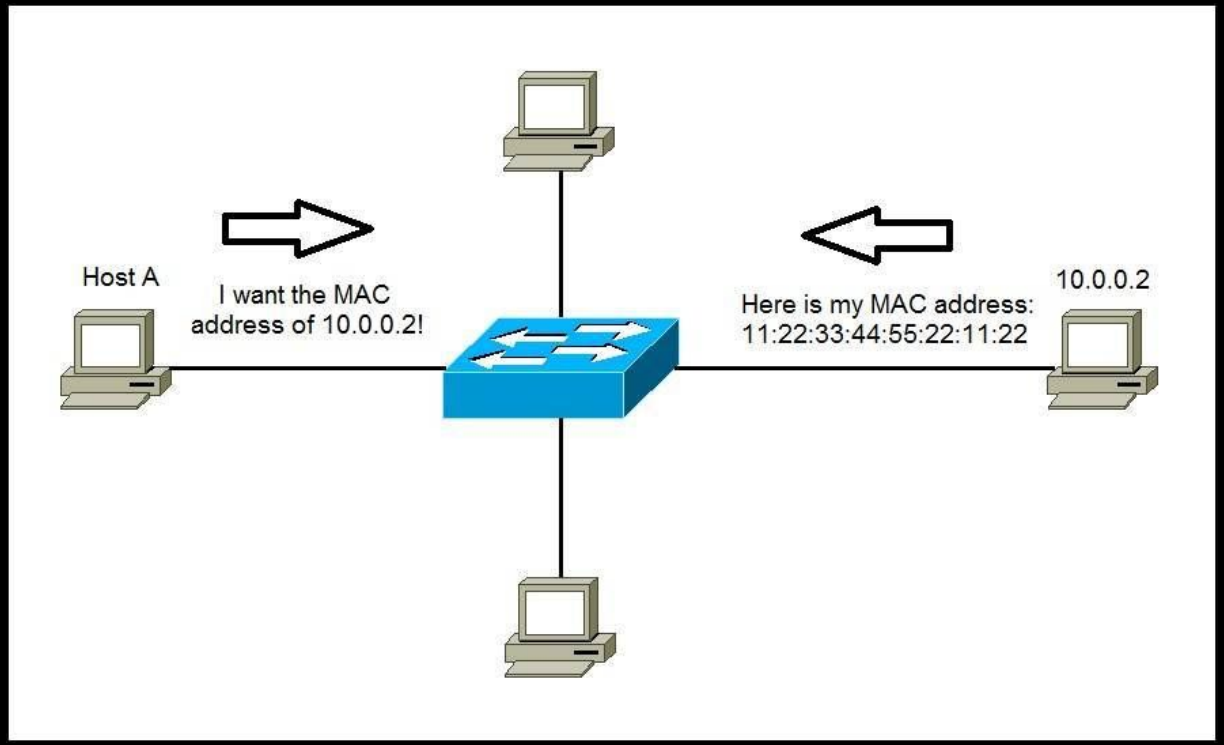
- 스니핑 공격의 탐지
  - 네트워크에 별다른 이상 현상을 일으키지 않기 때문에 인지하기 어려움
  - 스니퍼가 무차별 모드에서 작동한다는 점을 이용
- 스니퍼 탐지의 예시 (강의실에서 교수가 출석을 부를 때)
  - 친구의 출석을 대신 해주기로 한 학생은 자신의 이름이 호명되지 않았는데도 목소리를 바꿔서 대답
  - 두 명이 동시에 대답한다면 무차별 모드인 학생은 교수에게 들키게 됨



스니핑 공격

- 스니핑 공격의 탐지
  - ping을 이용한 스니퍼 탐지
    - 대부분의 스니퍼는 일반 TCP/IP에서 동작하기 때문에 request를 받으면 response를 전달
    - 이를 이용하여 의심이 가는 호스트에 ping을 보내면 스니퍼를 탐지
    - MAC 주소를 위장해서 전송
    - 만약 ICMP echo reply를 받으면 해당 호스트가 스니핑을 하고 있는 것
  - 유인을 이용한 스니퍼 탐지
    - 스니핑 공격을 하는 공격자의 주요 목적은 아이디와 패스워드 획득
    - 보안 관리자는 이 점을 이용하여 가짜 아이디와 패스워드를 네트워크에 계속 뿌림
    - 공격자가 이 아이디와 패스워드로 접속을 시도할 때 스니퍼를 탐지
  - ARP를 이용한 스니퍼 탐지
    - 위조된 ARP request를 보냈을 때 ARP response가 오면 무차별 모드로 설정되어 있는 것

ARP Protocol



ARP Spoofing/Poisoning

- ARP 스푸핑은 MAC 주소를 속이는 것
  - 로컬에서 통신하는 서버와 클라이언트의 IP 주소에 대한 MAC 주소를 공격자의 MAC 주소로 속임
  - 클라이언트에서 서버로 가는 패킷이나 서버에서 클라이언트로 가는 패킷이 공격자에게 향하게 하여 랜의 통신 흐름을 왜곡

Q&A